REMARKS

The Examiner is thanked for the thorough examination of the present application. The Examiner is also thanked for properly withdrawing his prior rejections. Dependent Claim 38 has been amended to address the minor informality as helpfully pointed out by the Examiner. The patentability of the claims is discussed below.

I. The Claimed Invention

The invention, as recited in independent Claim 1, for example, is directed to a cryptographic device that includes a cryptographic module and a communications module removably coupled thereto. The cryptographic module includes a first housing, a user Local Area Network (LAN) interface carried by the first housing, and a cryptographic processor carried by the first housing and coupled to the user LAN interface. The cryptographic module also includes a tamper circuit for disabling the cryptographic processor based upon tampering with the first housing. The tamper circuit includes at least one conductive trace printed on at least the inside of the first housing so that the cryptographic processor is disabled based upon a break in the at least one conductive trace. Furthermore, the communications module includes a second housing and a

network wireless LAN interface carried by the second housing coupled to the cryptographic processor and switchable between wireless LAN modes.

Independent Claim 11 is directed to a similar cryptographic device, and independent Claims 21 and 25 are directed to related methods. Independent Claim 29 is directed to a related communications system.

II. The Claims Are Patentable

The Examiner rejected independent Claims 1, 11, 21, 25, and 29 over Dhir et al. in view of Cheng in further view of Oldfield et al. Dhir et al. is directed to a programmable integrated circuit, namely a field programmable gate array (FPGA), that can be used to handle different wireless local area network (WLAN) communication specifications. The integrated circuit includes a transceiver coupled to programmable gates, memory coupled to the programmable gates for storing instructions for programming a first portion of the programmable gates with a selected one of a first type of a medium access layer and a second type of a medium access layer. The first type of the medium access layer is different from the second type of medium access layer, though both the first type of the medium access layer and the second type of the medium access

layer are compatible with the transceiver. The memory is configured for storing instructions for programming a second portion of the programmable gates as a baseband controller. (See, e.g., Col. 2, lines 14-49, of Dhir et al.).

The Examiner correctly acknowledges that Dhir et al. fails to teach a cryptographic module and a communications module that are removably coupled to one another, and a cryptographic module including a tamper circuit for disabling the cryptographic processor based upon tampering with the first housing. The Examiner then turned to Cheng for one of these critical deficiencies. Cheng is directed to an add-on card for a computer that is detachable from the computer and allows the computer to communicate with both wired and wireless networks. The add-on card includes an access control circuit, volatile and non-volatile memory, a wireless transmission module, and a network connection module. The network connection module has both an antenna for communicating with a wireless network, and a standard network cable port for connecting to a wired network. (See, e.g., paragraphs 0009-0010 of Cheng).

The Examiner still further recognized that even a selective combination of Dhir et al. and Cheng fails to disclose the cryptographic module including a tamper circuit for disabling the cryptographic processor based upon tampering with

the first housing, the tamper circuit including at least one conductive trace printed on at least the inside of the first housing so that the cryptographic processor is disabled based upon a break in the at least one conductive trace. The Examiner turned to Oldfield et al. for this critical deficiency.

Oldfield et al. is directed to an intrusion detecting electronic circuit package and includes a containment wall having a pair of conductors arranged in a rows and columns. Electronic circuitry within the containment wall includes a transmitter for transmitting signals in anti-phase relationship. A receiver receives the signals from the pair of conductors and a detector connected to the receiver detects any significant in-phase components or interruptions in the signals.

Applicants submit that the Examiner mischaracterized Oldfield et al. in that it fails to disclose the tamper circuit is for disabling the cryptographic processor based upon tampering with the first housing, and wherein the tamper circuit includes at least one conductive trace printed on at least the inside of the first housing so that the cryptographic processor is disabled based upon a break in the at least one conductive trace. Instead, Oldfield et al. merely provides an output tamper signal to indicate that tampering may have or is occurring. (See Oldfield et al. Col. 4, lines 8-10). Moreover,

Oldfield et al. discloses an encryption unit 160 including the electronic circuit for providing the tamper detectable package. (See Oldfield et al., Col. 5, lines 59-61). In other words, a break in one of the conductors would not disable the encryption unit 160 because the encryption unit includes the tamper detection circuitry.

Additionally, Applicants submit that the Examiner's combination of references is improper. More particularly, a person having ordinary skill in the art would not turn to Cheng to combine with Dhir et al. and Hamlin to arrive at the claimed invention. As an initial matter, Dhir et al. is directed to a programmable logic device for a WLAN. The communications module and the cryptographic module are purposely on a single circuit board (330), as illustrated in Fig. 8 of Dhir et al. Combining Dhir et al. with Cheng so that the communications module and the cryptographic module would be removably coupled would require splitting the communications and cryptographic modules from the single circuit board.

Moreover, using Cheng as a motivation to modify Dhir et al. would result in arbitrarily dividing the circuitry of Dhir et al. between the antenna 336 and the WLAN transceiver 301, the antenna being outside the circuit board and downstream from both the communications and cryptographic modules. This is

because Cheng discloses removably coupling the communications modules to a connector portion, including a physical connector and antenna. Accordingly, even if there was some proper motivation to combine Dhir et al. and Cheng, the claimed invention is not produced because the removable coupling is not between the communications module and the cryptographic module.

Still further, one of ordinary skill in the art would not turn to the security device including a spectral signal comparison data security system to combine with the programmable integrated circuit from Dhir et al. and the add-on card for a computer that is detachable from the computer and allows the computer to communicate with both wired and wireless networks from Cheng. In other words, the Examiner is attempting to combine an FPGA for a wireless LAN with a PCMCIA network add-on card and a device including cryptosystem validation.

Even still further, one of ordinary skill in the art would not turn to Oldfield et al. to further attempt to supply the deficiencies of Dhir et al. and Cheng. More particularly, a person skilled in the art would not turn to Oldfield et al., which is directed to an intrusion detecting electronic circuit package, to selectively combine with an FPGA for a wireless LAN an a PCMCIA network add-on card and a device including cryptosystem validation. Applicants submit that the Examiner is

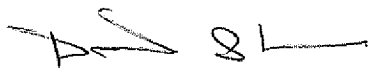
improperly combining disjoint pieces of the prior art in an attempt to arrive at the claimed invention, and that the Examiner's combination of references is improper.

Accordingly, it is submitted that independent Claims 1, 11, 21, 25, and 29 are patentable over the prior art. Their respective dependent claims, which recite yet further distinguishing features, are also patentable over the prior art and require no further discussion herein.

III. CONCLUSION

In view of the arguments provided herein, it is submitted that all the claims are patentable. Accordingly, a Notice of Allowance is requested in due course. Should any minor informalities need to be addressed, the Examiner is encouraged to contact the undersigned attorney at the telephone number listed below.

Respectfully submitted,



DAVID S. CARUS
Reg. No. 59,291
Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
407-841-2330
Attorneys for Applicants